ATLASOA LLC | ATLAS K-12

# Atlas K-12

IT Director Technical Packet
Windows-only deployment, local Compass AI

**FOUNDER PARTNER OFFER**

Year 1 free for founder partners.  ashleyreddick@atlasoa.com

**MTSS . COMPASS AI . ON-PREMISE . FERPA AND COPPA ALIGNED**

ashleyreddick@atlasoa.com | AtlasOA LLC | Missouri, USA

# Executive Summary

Atlas K-12 is an on-premises MTSS (Multi-Tier System of Supports) platform. It runs entirely on hardware your district already owns. It pulls from your SIS, unifies academic, behavior, attendance, and SEL data, and runs a local AI assistant (Compass) that never calls any cloud.

## THREE COMMITMENTS

- On-premise only. No cloud subprocessors. No telemetry. No outbound calls under normal operation. The product has no server-side component we operate.
- The Compass AI process has no outbound network access under normal operation. Compass is a local language model running on your hardware; student data is never sent to any external AI service.
- The district IT team is in full control. Atlas runs as Windows Services on a server you own, against a database that lives on your disk, behind your existing network boundary and your existing backup system.

## WHAT THIS PACKET COVERS

- Minimum system requirements for all three Compass tiers
- Three supported network architectures (Private WAN, Separate Building Internet, Air-Gapped)
- Security features that are built today and compliance alignment
- Pre-install checklist and Day-1 install summary
- SIS connection matrix and adapter guidance
- Update cadence and patch management



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

SYSTEM REQUIREMENTS

# Minimum spec by Compass tier

Atlas K-12 runs on a single Windows server. Compass AI tier determines the RAM and optional GPU requirement. All three tiers run on the same Atlas K-12 codebase: only the local model changes.

| Component | Compass Lite | Compass Standard | Compass Pro |
|---|---|---|---|
| Best for | Single school pilot | Small-to-mid district | Large district 7,500+ |
| Local model | Phi-3 Mini 3.8B | Mistral Small 3 24B | Llama 3.3 70B |
| RAM | 16-32 GB | 64-96 GB | 128-192 GB |
| CPU | Ryzen 5 / i5 6+ | Ryzen 7 / i7 8+ | Ryzen 9 / Threadripper / Xeon |
| GPU | Not required | Optional RTX 4060 Ti | Recommended RTX 4090 / A6000 |
| Disk | 500 GB SSD | 1 TB NVMe | 2 TB NVMe + backup volume |
| OS | Windows 10 / 11 (64-bit) | Windows Server 2019 / 2022 (64-bit) | Windows Server 2019 / 2022 (64-bit) |
| Network | 1 Gbps | 1 Gbps | 10 Gbps recommended |

## NOT REQUIRED

- Active Directory (SAML or OIDC is sufficient)
- Kubernetes or container orchestration (Windows Services do the job)
- External database (bundled SQLite works; Postgres supported but optional)
- Public internet exposure



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

# Pick the shape that fits your district

### Shape 1: Private District Network (LAN + VPN)

Best for most mid-size and larger districts. Atlas K-12 lives on a server in the district data closet. Every building reaches it across the existing private WAN. Off-campus staff reach it through the district's existing VPN. No public DNS. No public URL. Windows Firewall is the only perimeter control you need.

### Shape 2A: Separate Building Internet with VPN Tunnels

Best for rural, charter, and small districts where each building has its own ISP. Atlas lives at one building. Each other building runs a WireGuard or IPsec tunnel back to the host site. Vendor-agnostic: Meraki, FortiGate, SonicWall, Ubiquiti, and pfSense all work.

### Shape 2B: Public URL Behind SSO

Best for districts that want "just give me a URL" without running VPN tunnels. Atlas lives at one site with a static public IP. IIS terminates TLS and proxies to Atlas. Google Workspace or Microsoft Entra enforces SSO. Optional IP allowlist on the IIS site for extra defense.

### Shape 3: Fully Air-Gapped Single-Site

Best for districts with strict state DOE findings or post-ransomware policies that require zero remote access. No VPN. No public URL. Only in-building reachability. Compass model file is pre-staged via USB before the first boot.



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

SECURITY FEATURES BUILT TODAY

# What is actually in the binary

Atlas K-12 is founder-built software in active development. The table below lists the security features that are built and working in the product today. When more features land, they get added here, not before.

| Category | What is built today |
|---|---|
| Authentication | Local username and password accounts. 8-hour session timeout. Brute-force lockout after 5 failed attempts per IP in a 15-minute window. Single sign-on is scaffolded but not production-ready today. |
| Authorization | Role-based access control with four roles (teacher, counselor, admin, district admin) plus a Care Team coordinator flag. Per-school scoping. Per-record visibility checks on every route that takes a student identifier. |
| Data at rest | The database lives on your server. Full-disk encryption (BitLocker or equivalent) is the district IT team's call at the host level. Backups use your existing backup tooling. |
| Data in transit | TLS from browser to Atlas, terminated by IIS on your server. The Compass AI process has no outbound network calls under normal operation, enforced by a process-level socket guard inside the Python runtime. |
| Audit log | Every create, update, delete, and import operation is written to a local audit log with user, timestamp, and affected record. The log lives in your own database. There is no read-side access logging today. |
| Compliance | FERPA, COPPA, California SOPIPA, New York Education Law 2-d, Colorado HB14-1294, Connecticut SB949: alignment comes from the on-premise architecture, not from any vendor cloud. |
| Incident response | Atlas K-12 follows a shared responsibility model. The Educational Agency is responsible for runtime monitoring of the server, network perimeter, and audit log on its own deployment. AtlasOA LLC is responsible for code-level security, coordinated disclosure of any vulnerability that affects more than one customer, and 72-hour notification of any unauthorized access involving the Atlas K-12 codebase or AtlasOA vendor systems. The full division is documented in Section 4A of the Atlas K-12 Data Processing Addendum. |
| Patching cadence | Atlas K-12 itself is patched on a published cadence: critical security fixes within 7 calendar days of discovery, high-severity within 30 days, others bundled into the next monthly release. |
| Operational | On-premise only. No cloud subprocessors. No telemetry. Air-gap install option. Signed Windows installer built with Inno Setup and code-signed through Azure Trusted Signing. |

## WHAT THE DISTRICT IT TEAM OWNS

- Host hardening: OS patching, BitLocker, antivirus, Windows Firewall, and the rest of the district server baseline.
- Incident detection and response for any security event on district infrastructure. Atlas runs on the district's own hardware.
- Backups and restore testing. Atlas writes to a single data directory that drops into any existing backup system.
- User provisioning and offboarding inside the Atlas admin screen.



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

PRE-INSTALL CHECKLIST

# Before install day

- Server hardware provisioned to your Compass tier (see page 3).
- Windows Server 2019 or 2022 (64-bit) installed and patched.
- Static internal IP assigned and internal DNS entry `atlas.districtname.local` pointed at it.
- Domain admin account with local Administrators membership on the Atlas server for initial setup.
- SIS vendor, version, and credentials ready for the adapter configuration step.
- SSO IdP admin on standby to create the SAML or OIDC application.
- Backup target available (Windows Server Backup, Veeam, or equivalent).
- Firewall plan: TCP 443 inbound from staff subnets, outbound default-deny for the Compass service account.



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

DAY-1 INSTALL SUMMARY

# About 2 hours of active work

| Step | Action | Time |
|---|---|---|
| 1 | Run signed AtlasK12-Setup.exe (Inno Setup installer). Accept defaults. | 10 min |
| 2 | Set ATLAS_NETWORK_MODE system env var to lan or proxied via setx /M. | 2 min |
| 3 | Install Atlas K-12 as a Windows Service via windows_service_install.ps1. | 5 min |
| 4 | Apply windows_firewall.ps1 for default-deny outbound and scoped inbound 443. | 10 min |
| 5 | First-run setup wizard: create admin user, select Compass tier, accept EULA. | 10 min |
| 6 | Connect SIS adapter (credentials, endpoint, test pull). | 20 min |
| 7 | Configure SSO application in IdP, paste client ID + secret into Atlas. | 15 min |
| 8 | Smoke test from a teacher workstation in another building. | 10 min |
| 9 | Back up C:\ProgramData\AtlasK12\ using your existing backup tool. | 15 min |



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

SIS ADAPTERS

# Out-of-the-box connectors

| SIS | Adapter type | Notes |
|---|---|---|
| PowerSchool | REST API | Uses PowerQueries for attendance, grades, and behavior. |
| Infinite Campus | OneRoster 1.2 + REST | Grade passback optional. |
| Aeries | REST API | Includes medical alert filter out of the box. |
| Synergy | REST API + TeacherVUE token | Class list pull runs nightly by default. |
| eSchoolPlus | OneRoster 1.1 | Tuned for SunGard / PowerSchool hybrid districts. |
| Ed-Fi | Ed-Fi API 3.x | Recommended for state-reporting alignment. |
| OneRoster (CSV) | Nightly drop folder | Works with any SIS that emits OneRoster CSV nightly. |



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

# How the local AI is kept local

Compass is a local language model. It runs on your server. It does not call OpenAI, Anthropic, Google, or any other external AI service. No student data is ever sent to an outside AI vendor because there is no outside AI vendor in the loop.

## HOW THE OUTBOUND BLOCK IS IMPLEMENTED TODAY

- A process-level socket guard is installed at application startup inside the Python runtime that hosts Atlas K-12 and Compass.
- The guard blocks outbound network I/O from Atlas code paths under normal operation.
- The district IT team can apply the usual host-level controls: Windows Firewall outbound rules, service-account restrictions, and their existing network egress controls. Atlas does not replace those controls, it runs inside them.
- Districts that want an OS-level second layer can request the optional Windows Firewall hardening script (windows_firewall.ps1) from AtlasOA LLC and apply it to their server.

## WHAT IS NOT CLAIMED

- Atlas K-12 does not claim a kernel-level guarantee against a determined attacker who has already achieved code execution on the district server. A compromised host is a compromised host, regardless of any vendor's software.
- Atlas K-12 does not replace the district's network security perimeter. It is meant to sit inside it.

## FOR YOUR SECURITY REVIEWER

Under a mutual NDA, AtlasOA LLC can walk your security reviewer through the socket-guard implementation, the hardening script, and the current test coverage. We share exactly what is built, not aspirational architecture.



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

UPDATES AND SUPPORT

# What happens after install

- Updates are distributed as signed AtlasK12-Setup.exe files (Inno Setup with Azure Trusted Signing).
- Patches ride on your existing Windows Update cadence for the OS layer.
- Atlas K-12 itself is patched separately, once per month under normal operation, and within 72 hours for any security-critical fix.
- Direct founder support via ashleyreddick@atlasoa.com. No ticket portals, no tier-1 wall.
- Founder partners get a direct Signal or phone channel for urgent issues during the first year.



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

# What ships in hardening/

- windows_firewall.ps1: primary script. Windows Firewall (Advanced Security) rules for default-deny outbound and scoped inbound 443.
- windows_service_install.ps1: installs Atlas K-12 and the optional fetcher as Windows Services.
- egress_proxy.conf: optional local egress proxy configuration for the Option B isolation pattern.
- egress_proxy_filter.txt: hostname allowlist used by the egress proxy.
- README.md: full hardening reference including verification commands.

**Windows is the supported and tested target.** Atlas K-12 is a Windows-only product. The shipping artifact is a signed Windows EXE built from `installer.iss` via Inno Setup and code-signed through Azure Trusted Signing. We test every release against Windows 10, Windows 11, Windows Server 2019, and Windows Server 2022. That is the only path we support in the field.



AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

NEXT STEPS

# How to bring Atlas K-12 into your district

- Email ashleyreddick@atlasoa.com with your district name, size, and the one problem you most want to solve.
- Schedule a 30-minute discovery call with the founder.
- We sit with your team, learn how your current workflow actually runs, review your data, and build the solution to fit the way you already work.
- Confirm your Compass tier based on district size, and ship a server to the Atlas team (or spin one up yourself).
- Install and go live. Written training materials are delivered with the install. Total elapsed time from email to production is usually two to three weeks.

**Contact:** ashleyreddick@atlasoa.com | AtlasOA LLC | Missouri, USA